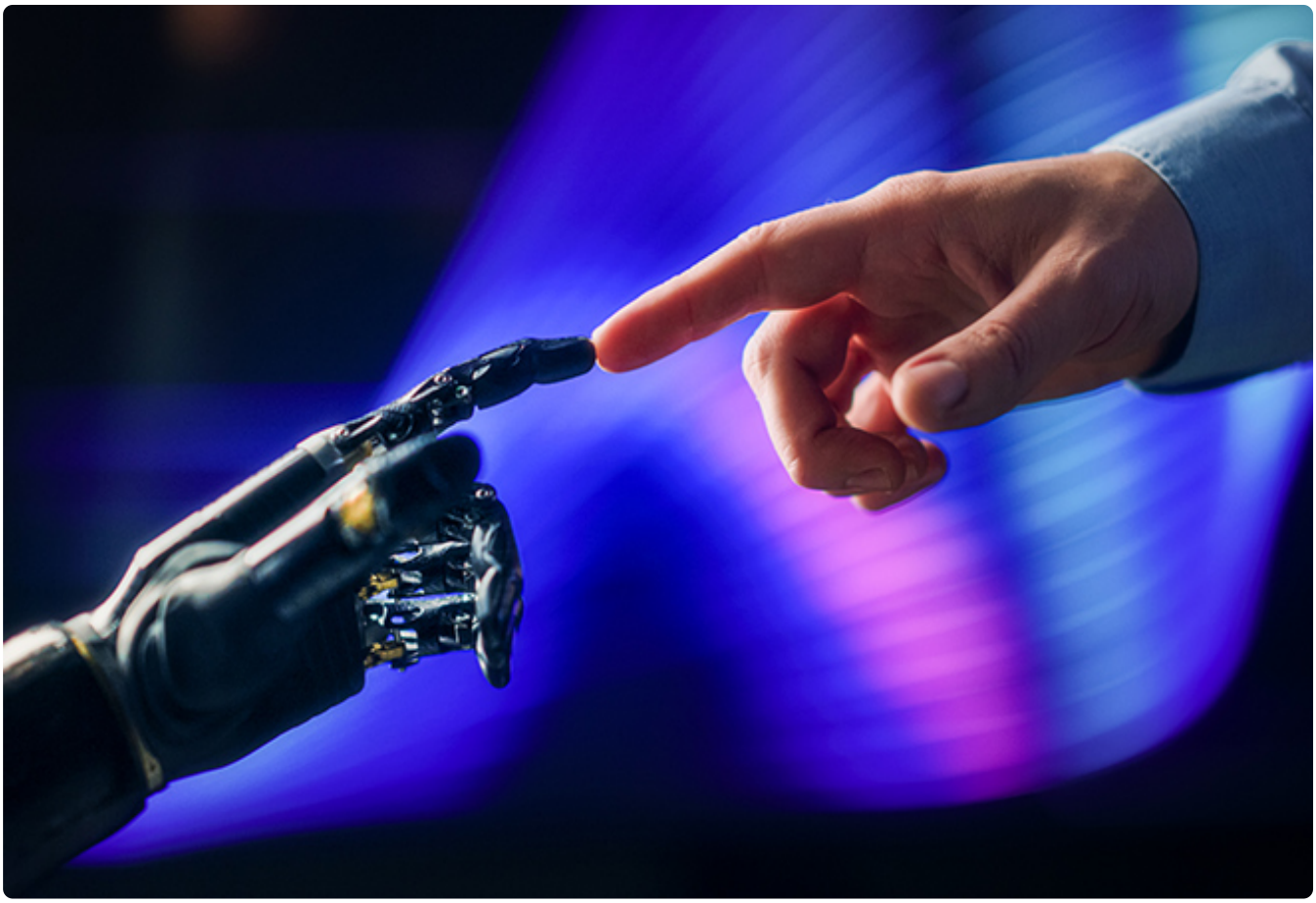
DIGITAL FRONTIERS | OCT 24 2020

Protecting enterprise secrets and intellectual property in a volatile world

GENIE SUGENE GAN

As technology evolves and new solutions emerge, governments have taken greater interest in regulatory matters, particularly in Indo-Pacific economies with nascent domestic tech industries.



iStock/Getty

COVID-19 | CYBERSECURITY INNOVATION | INDO-PACIFIC | NATIONAL CYBER SECURITY POLICY | PERSONAL DATA PROTECTION BILL | SUPPLY CHAINS

Digital technologies and the digitalisation of the economy and national security over the past two decades have ushered in new possibilities that have revolutionised business operations through integration and the seamless transfer of information in real time. This digital transformation has played a large role in leveling the playing field, allowing startups and smaller companies to scale rapidly and to disrupt established players. This metamorphosis has been most profound in the Indo-Pacific, where artificial intelligence (AI), blockchain technologies and cloud computing hold promise to guide some of the region's largest markets into digital leadership roles through the new 'Asian century' — a prospect largely unimaginable at the turn of the millennium.

As the digital landscape transforms with new innovative technologies, challenges have cropped up in tandem; cyber threats and zero-day exploits — from state-sponsored advanced persistent threats to opportunistic cybercriminals — result in costly intellectual property and data theft. Even single actors can pose grave threats to critical infrastructure, financial and logistics systems, and national security, endangering millions. These ever-present threats affect all industries, including healthcare, energy, transportation and retail, and necessitate constant vigilance, new security solutions and imaginative revaluations of the threat landscape.

> The advent of quantum computing may render traditional encryption obsolete, enabling bad actors to access encrypted data and sensitive information such as trade secrets.

Enterprise solutions such as endpoint security, cloud security and threat intelligence have enabled private and public sector entities to detect and keep ahead of such threats as they develop. Yet, new technologies have the potential to expose vulnerabilities and exploit digital weaknesses. The advent of quantum computing, for example, may render traditional encryption obsolete, enabling bad actors to access encrypted data and sensitive information such as trade secrets. While cybersecurity firms are exploring quantum resistant encryption as a stopgap measure, quantum computing may upend the entire cybersecurity landscape, precipitating a total rethink of its most basic tenets.

There has been additional impetus to evolve the current security culture's focus on confidentiality, integrity and availability to account for issues such as online abuse, harassment, disinformation and radicalisation. As the scope of cybersecurity expands, so too will the drive to define and proscribe this kind of behaviour. The development will spark debates on when intervention is acceptable and when it violates personal freedoms, feeding into larger conversations on tech values, ethics and regulation.

> Cybersecurity innovation will not able to address all challenges.

Nevertheless, cybersecurity innovation will not able to address all challenges. As technology evolves and new solutions emerge, governments have taken greater interest in regulatory matters, particularly in Indo-Pacific economies with nascent domestic tech industries. Technology companies must learn to work with regulators to strike a balance between data management and data governance on the one hand and ensuring a fertile environment for continued growth — involving streamlined and uniform regulations — on the other.

Companies must also be mindful that 21st century geopolitics will play a dominant role in shaping cybersecurity decisions and regulations. In the Indo-Pacific, strategic decoupling and shifting supply chains — trends already in motion well before COVID-19 — will accelerate the transformation of the digital landscape, as diversification opens new opportunities for Indo-Pacific countries. Companies in the region may also find themselves pitted between strategic competitors in choosing technology frameworks, security regimes and shared values. Remaining neutral may no longer be an option, as the route chosen will have consequences for societies, businesses and people. The trust of governments, companies and consumers has become an essential ingredient for sustainability and transparency; a hallmark of success.

> Remaining neutral may no longer be an option, as the route chosen will have consequences for societies, businesses and people.

This paper explores the landscape of cyber security in Asia Pacific, increased regulations, decoupling and supply chain disruptions, and the geopolitisation of security. It will touch on various challenges in addressing the evolving cyber security landscape in the Asia Pacific region, with a spotlight on India, and discuss how enterprise solutions can help companies overcome the challenges that lie ahead.

Megatrends in encryption and cybersecurity

Increased regulation

In response to the largely unrestrained technology boom over the last two decades, there has been a surge in regulation from governments desperate to exercise control over tech firms that have until recently operated with relative impunity. This is no different in the Indo-Pacific, where countries have adopted regulations to control the flow of information — often for national security purposes — to prevent and punish cybercrime; capture lucrative rents; and allow for fair competition, market access and the growth of domestic tech industries.

> Burdensome cybersecurity legislation can also compromise personal data and information privacy.

But technology is evolving fast and regulators are having difficulty keeping up, resorting to hasty legislation that can be harmful to the tech industry. Such was the case with Indonesia's GR 82 data localisation regulation, which was eventually amended by the less restrictive GR 71. Burdensome cybersecurity legislation can also compromise personal data and information privacy. In 2019, Australia passed the Assistance and Access Act, which allows the government to view encrypted information and requires firms to create "backdoors" to grant access. The

Indian government is now entertaining a similar legislation [1] that may threaten or even outlaw end-to-end encryption, undermining data privacy and leaving the biometrics and other personal information of over a billion people unprotected.

Though tech companies have tried to lobby for regulations favourable to the industry, their absence from policy consultations has sometimes resulted in regulation that may stymie growth and innovation in the tech sector. The emergence of a balkanised patchwork of conflicting regulations from different jurisdictions further complicates compliance and highlights the need for a common framework that advances the interests of all parties involved. Former Japanese Prime Minister Shinzo Abe articulated such a vision in the 2019 G20 summit, where he proposed [2] uniform rules on data sharing and data governance.

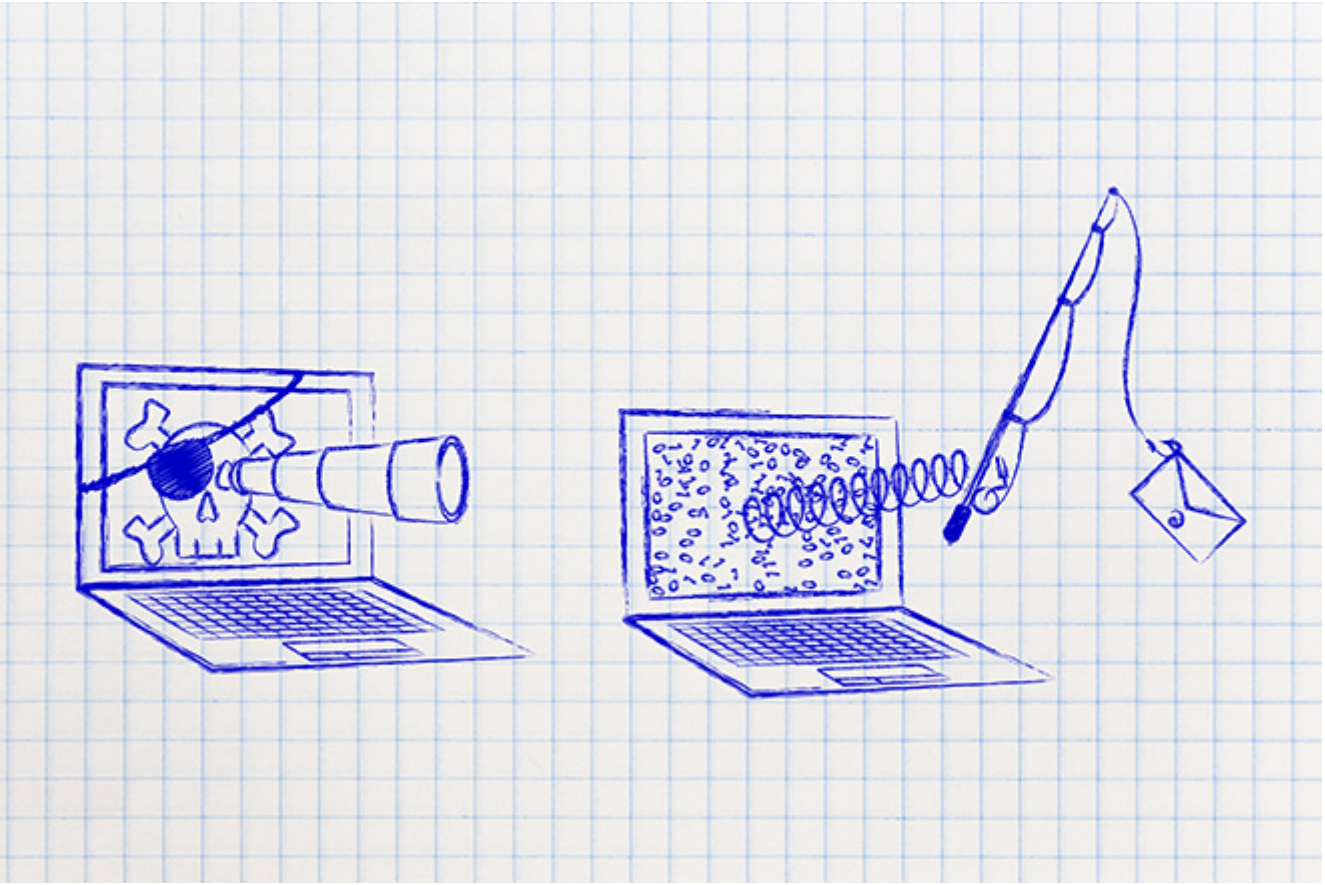
> The emergence of a balkanised patchwork of conflicting regulations from different jurisdictions complicates compliance and highlights the need for a common framework.

Regardless of whether this vision will come to pass, the consultative process will become increasingly important to take into account the considerations of all stakeholders and develop sound and enduring policies. In the meantime, security firms [3] will do well to keep clients abreast of new legislation so they are aware [4] of the environment in which they operate, ensure compliance and make adjustments to their investment calculus.

The expanded scope of cybersecurity amidst a pandemic

Cybersecurity firms have been diligent in offering a suite of enterprise solutions to combat the proliferation of traditional cyber threats such as malware, fraudulent activities and denial-of-service attacks. However, the ongoing pandemic has given rise to increased COVID-19-related phishing activity and lured many unsuspecting people into downloading malware to an extent greater than before. For example, there was a COVID-Antivirus website that offered people an executable Trojan instead of an anti-virus solution. And there were other groups that offered a fake World Health Organization (WHO) application to infect home routers and stage man-in-the-middle attacks (DNS Hijacking), and sent attachments with fake WHO information about a COVID-19 vaccine.

Based on Kaspersky's recent data, from January to July 2020, almost half (48 percent) of our users encountered a cyber threat. That is almost two billion cases among our user base, or 205 million malicious files. Compared to last year, we detect 25 percent more unique malicious files a day. That is 428,000 new threats a day.



The ongoing pandemic has given rise to increased COVID-19-related phishing activity and lured many unsuspecting people into downloading malware to an extent greater than before. Illustration: iStock/Getty

An inevitable result of the pandemic is the prevalence of lockdowns in almost every city in the world, resulting in people having to work from home on unsecure networks. In the months since the pandemic started, Kaspersky detected 600 million attempts to attack internet of things (IoT) devices, such as routers or cameras, and a 23 percent growth of brute-force attacks on database servers due to remote working.

Decoupling and supply chain disruptions

COVID-19 has accelerated the pace of decoupling and highlighted the importance of supply chain diversification — developments that were already in motion since the geopolitical kerfuffle of a US-China trade war. In the Indo-Pacific, companies are exploring ways to mitigate risk as they relocate assets from China to other countries in the region, with Vietnam attracting a large share of investments. The digitalisation of supply chains and logistics systems is one method of managing such risk, and countries in the Indo-Pacific are already exploring this option as they scramble to attract investment. In Indonesia, the Minister of State-Owned Enterprises Erick Thohir has called [5] for the digitalisation of supply chains to gain access to new markets and kickstart the county's economic recovery, while Japan [6] is trying to woo their companies to shift production away from China, as the pandemic exposed overreliance, and the Make In India campaign is a chance to restart India's high-end manufacturing growth story.

> In the Indo-Pacific, companies are exploring ways to mitigate risk as they relocate assets from China to other countries in the region, with Vietnam attracting a large

> share of investments.

But digitalisation carries risks of its own that must be addressed to ensure sustainability. As Vietnam becomes a more attractive destination for companies looking to shift their supply chains, it becomes ever more important that the integrity of its digital logistics systems is safeguarded. Thankfully, blockchain technology has the ability to optimise [7] and provide for the security of supply chains [8] and ensure the protection of data critical to their functionality. In Vietnam, the Ministry of Information and Communications is promoting digitised supply chains under the national digital transformation plan, and the country [9] is already developing indigenous blockchain technologies, like its recently unveiled akaChain, with an eye toward supply chain management.

While Japan [10] and Singapore have recognised the value of blockchain to the logistics sector for some time, the Indian government [11] is just starting to consider its potential. During the India Ideas Summit in July 2020, Prime Minister Narendra Modi encouraged investment in blockchain technology, dispelling concerns that India's early aversion to cryptocurrencies meant blockchain was off limits. As India [12] looks to attract investment from companies interested in diversifying supply chains, it may need to digitise logistics, secured with blockchain, to remain competitive.

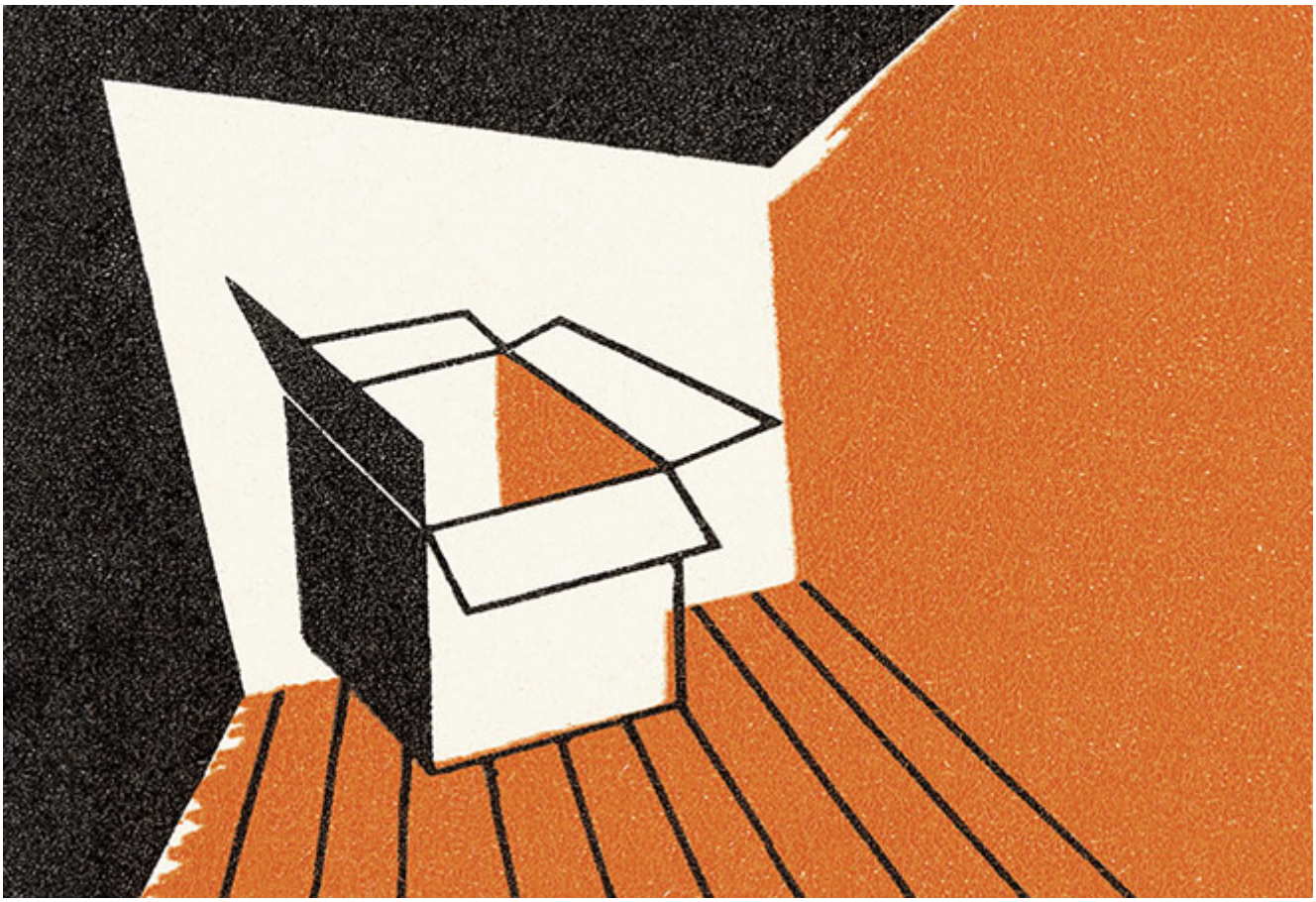
> Digitalisation carries risks of its own that must be addressed to ensure sustainability.

The digitalisation of supply chains and the application of blockchain technologies will require countries to adopt legislation that accommodates the changing tech landscape while providing for its security. As technology plays an increasingly large role in managing critical infrastructure, appropriate safeguards will need to be put in place to make sure the advantages to be gained through digitalisation do not come at a terrible cost.

Although the use of industrial control system (ICS) computing has done much to streamline critical infrastructure management — from energy and aerospace facilities to sewage systems — it has greatly increased the susceptibility of such systems to malicious cyber attacks. In 2019, Kaspersky detected over a hundred vulnerabilities in industrial, industrial IoT (IIoT) and IoT solutions. If exploited, these vulnerabilities could pose grave threats to national security, particularly for countries that have a greater dependence on ICS technology.

The looming threat of denial-of-service attacks, remote code execution, session hijacking and zero-day exploits demands robust IIoT solutions that ensure the integrity of critical infrastructure. As of H2 2019, only 39 percent of cyberattacks are blocked on ICS computers globally, though countries in the Asia Pacific tend to be more resistant, with Southeast Asia blocking 55.2 percent and South Asia 48.8 percent. Nevertheless, many Asian countries face a higher volume of ICS attacks than their peers, with Bangladesh, Vietnam, Indonesia, India, Malaysia and Thailand ranking among the most targeted countries. Ransomware is perhaps the single biggest threat to ICT, and less than one percent of attacks in 2019 were blocked on

all systems globally. Southeast Asia ranks the most resilient to ransomware, though it only blocked around 2.1 percent of all attacks, while South Asia blocked 1.7 percent of attacks.



The digitalisation of supply chains and logistics systems is one method of managing risk. Illustration: CSA Images/Getty

The devastating potential of ICS attacks were clearly illustrated in September 2019, when malware was discovered on India's Kudankulam nuclear power plant and was likely transmitted through a phishing attack. [13] The Kudankulam plant's administrative network was infected with the Dtrack malware, which allows attackers to access user credentials that may place them in total control of the nuclear power plant, a very precarious situation.

Geopolitisation of security and values

Governments are increasingly wielding technology for narrow strategic purposes such as defense and security, placing geopolitics at the center in technology discussions. In fact, values form a common thread through all of the above trends in cybersecurity and can have a major influence on their trajectories. Values dictate whether the powers of quantum computing will be used for good or to undermine security in the region; they also inform regulations, where a divergence of values is anathema to regulatory harmony. Values propel disinformation campaigns and determine whether authorities will pursue measured responses that preserve freedom of expression. Above all, values shape the environment in which technology operates and have enduring consequences for societies and people.

> Values dictate whether the powers of quantum computing will be used for good or to undermine security.

In today's geopolitics, it is not uncommon for state actors to hide behind technology and security companies, and use technology for nefarious purposes. They engage in industrial espionage and intellectual property theft, violate data privacy and conduct mass surveillance on their people. While in the past, it was assumed that tech companies could remain independent of the countries in which they operate in, this is clearly no longer the case. Tech and security companies are now expected to articulate the values to which they subscribe and make assurances that they are not extensions of state security apparatuses.

Transparency has become the currency of trust-building and the building blocks of sustainable partnerships at the business and diplomatic levels. In today's ultra-connected world, cybersecurity is no longer simply about protecting hardware and software, but about safeguarding digital governments, economies and everyday lives, and the vast volumes of data they create. If others do not believe they can trust you with their digital data, devices, networks and infrastructure, they will go elsewhere or will put up barriers to reduce any potential risk. Cybersecurity companies need to embrace transparency and demonstrate their commitment to it. This includes accepting the potential risks associated with making source code or processes accessible for review by trusted third-parties.

> If others do not believe they can trust you with their digital data, devices, networks and infrastructure, they will go elsewhere or will put up barriers to reduce any potential risk.

Spotlight: India

India has seen a rapid proliferation of Internet users with over 550 million users [14], which is expected to increase to 800 million in the next two years, largely fueled by increased rural and mobile phone penetration. The next billion internet users will come from Asia, and the Indian government aims to establish the country as a major presence in the global digital economy setting a digital economy target of US$1 trillion by 2024. [15]

Both the government and private sector are moving towards enhancing the use of new technologies and integrating them in delivering services to citizens and customers. All efforts are being made to set up hardware and services infrastructures to enable Indian consumers and businesses to get online. India's startup sector is now vibrant with seven unicorns — a few with Decacorn potential — and the best 200 fintech units also being housed in India. The government's Digital India initiative has also been driving the adoption of technology, from the use of digital payment systems to the adoption of cloud computing, 5G, e-commerce, and the recognition of new and emerging technologies like AI, machine learning and blockchain. With this proliferation of digitisation, challenges have also emerged in the regulation and protection of online spaces.

Cyber security landscape

With increased internet penetration and digitalisation, India's public and private sectors are vulnerable to cyber attacks, cybercrimes and incidents. Ongoing geopolitical tensions with neighbouring countries such as China and Pakistan, as well as emerging challenges from

working from home due to the COVID-19 pandemic, have seen an increase of almost 200 percent [16] in cybercrimes and cyber incidents of all types in India on both public and private sector facilities from state and non-state actors.

> Heterogeneous interfaces, improper configurations, vulnerabilities in hardware and software, and lack of processes will result in more cyber incidents and cyber crimes.

Advanced digitisation of supply chains and logistics systems, and the introduction of technology-enabled solutions, cloud computing, AI and data analytics will also result in increased vulnerabilities to cyber attacks. Heterogeneous interfaces, improper configurations, vulnerabilities in hardware and software, and lack of processes will also result in more cyber incidents and cyber crimes.

As India seeks to become a manufacturing intensive digital economy, protecting vital infrastructure against cyber attacks will be crucial to ensure growth and success. Companies would need to look at their existing infrastructure and invest in the right systems. The government, while considering the adoption of new technologies, would also need to make significant investments in shoring up the security of critical infrastructure to protect information security.

The private sector has also started increasing its role in managing and operating critical information infrastructure, including in power transmission, transportation, and healthcare. Keeping in mind the current global cyber security landscape, both from a regulatory and vulnerabilities point of view, companies are investing in building stronger defense mechanisms. There is an increased demand for robust security systems; in fact, India's cyber security services industry is estimated to grow at a compound annual growth rate (CAGR) of 20 percent to 22 percent [17] from FY2017-FY2025.

New cyber security challenges

India's emerging supply chain

India has the potential to fast become an attractive destination for companies to set up manufacturing units. In this regard, the Indian government has taken several measures to attract foreign investors, such as launching production-linked incentives, and creating technologies and infrastructure parks for large manufacturing units in electronics and pharmaceuticals. The government has announced a vision of a self-reliant India — *Atmanirbhar Bharat* — which will need to be fueled by increased investments in not just physical infrastructure but digital capabilities as well. The increased investment flows in the technology sector will also result in questions and concerns on the privacy and protection of data generated through online services, spurring legislation to regulate data flows.

The government has announced a vision of a self-reliant India — *Atmanirbhar Bharat* — which will need to be fueled by increased investments in not just physical infrastructure but digital capabilities as well. Photo: Mayur Kakade/Getty

Technologies like AI and machine learning can play a larger role in cyber security. Machine learning models that can predict and accurately identify attacks will be a boon to cyber security professionals. However, there is a risk that these systems may be exploited by attackers and used in a reverse manner. With the increased government focus on boosting India's domestic manufacturing capabilities and attracting investments in sectors such as electronics manufacturing, pharmaceuticals, medical devices amongst others, there is an increased threat of cyber attacks on vulnerable systems in the supply chain. The manufacturing of backdoors and embedding for hardware tampering will become common occurrences. Such complex embedded small and tiny systems will target network systems, banking systems and industrial control systems of manufacturing units.

COVID-19 changing the security landscape

The spread of COVID-19 in India has led to new and emerging challenges in securing online systems. With lockdowns to prevent the spread of the pandemic, companies have had to shift to work-from-home models of operations. Work-from-home has now become the norm and the center of all activity, including education, work and financial transactions. IT infrastructures, which were meticulously crafted to secure online systems at offices, have now had to cope with a scattered workforce and workspace. Unsurprisingly, hacks on vulnerable systems have increased since the start of the pandemic in India and during subsequent lockdowns. The use of contact tracing apps to detect COVID-19 positive individuals has also given rise to security threats and breaches.

> IT infrastructures, which were meticulously crafted to secure online systems at offices, have now had to cope with a scattered workforce and workspace.

Cybercrimes have largely targeted citizens' wallets and personal data. Several fraudulent techniques and portals have been launched relating to the coronavirus to lure people to make donations to COVID-19 funds. A primary example of this was the creation of fake versions of the 'PM CARES Fund' soliciting thousands of dollars from individuals and organisations [18] Personal data also remains an attractive target, with increased malware and phishing schemes launched under false pretenses of COVID-19 prevention efforts, aimed at stealing bank details, passwords and other sensitive information.

Cybercrimes have not only been targeted towards individuals, but have targeted key sectors such as defense, health, processing and other sectors relating to national security. Cert-In, India's cyber security nodal agency, has issued several advisories since March 2020, warning users of phishing and malware attacks, and issuing guidelines on protection against cyber incidents and attacks. The government has recently also advised the private sector to undertake security audits to evaluate their infrastructure and human resource capabilities to prevent and manage attacks.

India's cyber security regulatory framework

Along with advances in technology, there is also an increased focus on regulation. Over the last few years, India has seen a rapidly emerging regulatory environment for data protection and governance. The focus on data privacy is likely to reach a tipping point, with the passage of the draft Personal Data Protection Bill, currently under review by a joint parliamentary committee.

The government has, in recent years, also moved towards taking a tougher stance on the spread of misinformation on digital platforms, and the need for increased accountability by online platforms when it comes to national security and cooperation with security agencies. Data sovereignty has become a key approach in forming policies to protect the data rights of citizens, as well as for security agencies to effectively track and trace any breaches.

> Compliance requirements under the regulatory frameworks, along with a risk to reputation from any data breaches, are expected to drive these investments.

Regulatory requirements are becoming more stringent, as evidenced by the Personal Data Protection Bill [19], DISHA [20], the Supreme Court of India's ruling on the Aadhaar Act [21], and amendments to liabilities of online intermediaries under the IT Act. [22] This increased regulatory focus is leading to a demand for compliance, and companies are likely to focus on making increased investments in data security and privacy systems, including end-point security. Compliance requirements under the regulatory frameworks, along with a risk to reputation from any data breaches, are expected to drive these investments.

The Asia Pacific's digital transformation has led to the exponential growth of online business models; rise of online banking, e-payments and fintech; proliferation of mobile phones and other smart devices; and expansion of cloud computing and other technologies. However, the embrace of IoT has also exposed significant vulnerabilities that threaten the region's burgeoning digital economy. Moreover, as the COVID-19 pandemic and the transition to remote work accelerate the pace of digitalisation — with over half of Indian firms [23] expected to increase cloud use — cyber threats have grown in tandem. As such, governments, businesses and tech consumers are becoming increasingly cognisant of the need to protect their data — a trend reflected in the surging demand for endpoint security in the Asia Pacific. According to a Mordor Intelligence report, [24] there will be an 8 percent CAGR for endpoint security between 2020 and 2025, and Asia Pacific will lead the way as the fastest growing market.

> The embrace of IoT has exposed significant vulnerabilities that threaten Asia Pacific's burgeoning digital economy.

Regulatory institutions like India's central bank, the Reserve Bank of India, through various announcements, and the Securities and Exchange Board of India are also taking cognisance of evolving risks from technological advancements.

National cyber security strategy

Currently the Information Technology Act 2000 is the primary law for dealing with transactions in the cyber space. A National Cyber Security Policy was developed in 2013 with the express purpose of building a secure and resilient cyberspace for Indian citizens and businesses. The purpose of this policy was to protect information and information systems, build and develop capabilities to prevent and respond to cyber attacks, reduce vulnerabilities from cyber incidences through institutional structures, people, processes, and technological capabilities. An updated strategy was released in 2019 is expected to be formalised by the government soon.

Improving cyber security systems in India: Challenges and opportunities

Cyber security governance structures in India are currently fractured, and at times operate in silos. There is also a lack of coordinated and structured information sharing mechanisms between the government and the private sector. India's new cyber security strategy can seek to address these gaps by streamlining coordination between government agencies, creating a centralised system of governance.

> Governments and companies will need to invest not only in hardware and software capabilities, but also training of manpower to operate and manage such complex systems.

It is also imperative that while information sharing is improved within government agencies, this system must also be expanded to cover the private sector. Processes that seek to improve disclosures of security vulnerabilities must be clearly defined and operationalised.

AI, quantum computing, machine learning, the influx of IoT devices and increased digitisation have only complicated the security infrastructure. Governments and companies will need to invest not only in hardware and software capabilities, but also training of manpower to operate and manage such complex systems. India has a vast talent pool that can be tapped into to create a resilient cyber infrastructure.

Endnotes

[1] Amit Yoran, "Australia's Assistance And Access Bill Increases Risks Of Cyber Attacks", *Forbes,* February 25, 2019.

[2] Casey Newton, "India's proposed internet regulations could threaten privacy everywhere", *The Verge*, February 14, 2020.

[3] Samm Sacks and Sherman Justin, "The Global Data War Heats Up", *The Atlantic,* June 26, 2019.

[4] "Kaspersky Lab opens new Transparency Center in Madrid and conducts independent legal assessment of Russian legislation related to data-processing", *Kaspersky,* April 2, 2019; "On Cybersecurity Laws – and Their Interpretations", Kaspersky, September 2, 2019.

[5] Juwita Trisna R and Sri Haryati "SOE Minister Thohir encourages digitalization of logistic supply chain", Antaranews.com, 15th August 2020.

[6] Simon Denyer, "Japan helps 87 companies to break from China after pandemic exposed overreliance", The Washington Post, July 21, 2020.

[7] Anthony B Kerr, "COVID-19: (Asia Pacific) Renaissance of the Supply Chain", KL Gates, 12 May 2020.

[8] Josh Schultz, "The Role of Cryptography in Procurement and Supply Chain", Medium, December 26, 2017.

[9] Tran Binh, "Make-in-Vietnam blockchain platform akaChain launched", *Saigon GiaiPhong Online,* August 14, 2020.

[10] Christophe Ozer, "Logistically sound: Japan's digital supply chain future", *Orange Business Services*, August 19, 2019.

[11] Martin Young, "Indian PM Backs Blockchain as 'Frontier Technology'", *Cointelegraph*, July 24, 2020.

[12] Akshobh Giridharadas and Vaman Desai, "After COVID–19: Manufacturing India's New Economic Potential", *The Diplomat,* April 29, 2020.

[13] Mint, "India confirms malware attack at Kudankulam nuclear power plant," *Livemint*, November 20, 2019.

[14] "Digital India", *McKinsey Global Institute*, March 2019.

[15] Shruti Srivastava, "India Targets to Triple Exports to $1 Trillion in Next 5 Years," *Bloomberg*, September 12, 2019.

[16] "200% increase in cyber incidents in two months, but not attributable to China: Official", *The Economic Times*, July 07, 2020.

[16] "India Cybersecurity Services Landscape- A Global Hub in the Making", *DSCI*, May 21, 2020.

[17] Tech Desk, "Fraudsters using fake PM CARES FUND links to dupe people; don't fall for it," *The Indian Express*, April 5, 2020.

[18] Suneeth Katarki et al., "The Personal Data Protection Bill, 2019: Key Changes And Analysis," *Mondaq*, January 6, 2020.

[19] Rahul v Pisharody, "Disha Bill: What are the highlights of Andhra Pradesh's new law?", *The Indian Express*, December 14, 2019.

[20] ET Online, "What's valid and what's not: Everything you need to know about Aadhaar verdict," *The Economic Times*, September 26, 2018.

[21] Tanya Sadana , Anirudh Rastogi and Aman Taneja, "Impact Of Proposed Amendments To Intermediary Guidelines," *Mondaq*, May 12, 2020.

[22] "64% of the Indian Organizations Expect to Increase Demand for Cloud Computing, as a Result of COVID-19, Says IDC", *IDC*, June 2, 2020.

[23] "Endpoint Security Market – Growth, Trends, and Forecast (2020-2025)", *Mordor Intelligence.*

[24] "Will soon unveil a new cyber security policy: PM Modi", *The Times of India*, August 15, 2020.

About ORF

Set up in 1990, ORF seeks to lead and aid policy thinking towards building a strong and prosperous India in a fair and equitable worl
Indian voices and ideas to forums shaping global debates. ORF provides non-partisan, independent analyses and inputs on matters o
resources and global governance to diverse decision-makers (governments, business communities, academia, civil society). ORF's ma
platforms and invest in tomorrow's thought leaders today.

Topics

Climate, Food and Environment

Defence and Security

Development

Development Partnerships

Domestic Politics and Governance

Economics and Finance

Energy

Gender

Healthcare

International Affairs

Media and Internet

Content Type

Videos

Series

Books and Monographs

Commentaries

Event Reports

GP-ORF Series

Issue Briefs and Special Reports

Monitors

Occasional Papers

Primer

Archives

Programmes

Strategic Studies

Tech and Media

Energy

Climate Change and Sustainable Development

Economy and Growth

Political Economy

Initiatives

Cybersecurity and Internet Governance

Education and Skilling

Energy and Resources

Eurasian Studies

Future of Work

International Trade and Finance

Maritime Studies

Media Studies

Neighbourhood Studies

Nuclear and Space Studies

Political Reform and Governance

Public Health

Urban Policy

Geographies

Africa

Americas

China

European Union

India

Neighbourhood

Russia and Eurasia

The Pacific, East and Southeast Asia

USA and Canada

West Asia

Who We Are

Work With Us

Write For Us

Media Inquiry

Partners

Subscribe To ORF

Contact Us